T_Open

Securely specify and protect target filename.

Sean Barnum, Cigital, Inc. [vita[1]]

2007-04-23

Part "Original Cigital Coding Rule in XML"

Mime-type: text/xml, size: 3356 bytes

Attack Category	• Path spoofing or confusion problem
Vulnerability Category	• Indeterminate File/Path
Software Context	• Networking
Location	• xti.h
Description	The t_open() function must be called as the first step in the initialization of a transport endpoint. This function establishes a transport endpoint by supplying a transport provider identifier that indicates a particular transport provider (that is, transport protocol) and returning a file descriptor that identifies that endpoint. The argument name points to a file name that identifies a transport provider. If the communication is potentially sensitive, then it is important that no untrustworthy party can specify the file name or substitute an unauthorized file or device corresponding to the specified name.
APIs	**Function Name** / **Comments** t_open
Method of Attack	If an attacker can specify an unauthorized file or device, the program could be made to communicate insecurely. The attacker could tamper with or monitor the communication.
Exception Criteria	
Solutions	**Solution Applicability** / **Solution Description** / **Solution Efficacy** Whenever t_open is used. / For the communication to be secure, the filename passed to t_open() must be specified in a secure fashion, and the / Effective with respect to the identified issue, though other communication vulnerabilities may still exist.

1. http://buildsecurityin.us-cert.gov/bsi/about_us/authors/35-BSI.html (Barnum, Sean)

		referenced file or device must be secured from tampering.	

Signature Details	int t_open(const char *name, int oflag, struct t_info *info);
Examples of Incorrect Code	`int fd = t_open(insecurelySpecifiedName, flag, info);`
Examples of Corrected Code	`int fd = t_open("/dev/securedNameForSecuriedDevice", flag, info);`
Source References	• ITS4 Source Code Vulnerability Scanning Tool [2] • http://seclab.cs.ucdavis.edu/projects/vulnerabilities/scriv/ucd-ecs-95-09.pdf [3]
Recommended Resource	• man page for t_open() [4]
Discriminant Set	**Operating System**: • UNIX **Languages**: • C • C++

Cigital, Inc. Copyright

1. mailto:copyright@cigital.com